UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/530,075	08/30/2005	Johan Rune	P17191US1	7540

27045 7590 04/02/2009

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
CRUTCHFIELD, CHRISTOPHER M	
ART UNIT	PAPER NUMBER
2419	

MAIL DATE	DELIVERY MODE
04/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/530,075	RUNE, JOHAN	
	Examiner	Art Unit	
	Christopher Crutchfield	2419	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *6,8,10-12,18,19,21-23 and 26-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *6,8,10-12,18,19,21-23 and 26-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. **Claims 6, 8, 18 and 19** rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Applicant's specification provides no support for assigning a dedicated uplink to each host for carrying uplink traffic to the access router (As required by claims 26 and 27) while simultaneously also assigning one uplink VLAN for each Access Point (AP), each uplink VLAN for carrying uplink traffic from an associated AP and the hosts connected to the associated AP to the access router (As required by claims 6 and 18). This appears to be an accidental combination of features from the applicant's second embodiment for fixed access networks (See The Pre Grant Publication, No. 2006/0062187, of the Applicant's Specification, Paragraphs 0116-0127) wherein each host (as opposed to access point) is connected to an individual switch port and receives a separate asymmetric uplink VLAN (See The Pre Grant Publication, No. 2006/0062187, of the Applicant's Specification, Paragraphs 0116-0127) with the applicants second embodiment for Isolating Hosts Connected to WLAN Access Networks, wherein each Access Point (as opposed to host) is connected to a port of the switch and is assigned a single asymmetric uplink VLAN for communicating with the router (See The Pre Grant Publication, No. 2006/0062187, of the Applicant's Specification, Paragraphs 0110-0115).

2. **Claims 6, 8, 18 and 19** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

A person of ordinary skill in the art, upon reading the specification would not have been able to make or use an invention that implements both the per host asymmetric uplink VLANS of Claims 26 and 27 (See Claims 26 and 27) and the per access point asymmetric uplink VLANs of Claims 6 and 18, (See Claims 6 and 18) as the requirements are conflicting, requiring a single uplink VLAN from each access point to the router, but also requiring the same traffic to be a member to the multiple independent asymmetric host VLANs for each host.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. **Claims 26 and 27** are rejected under 35 U.S.C. 103(a) as being unpatentable over *Edsall*, et al. (US Patent No. 6,741,592 B1) in view of The Cisco 7600 Optical Services Router Software Command Reference (Author Unknown, The Cisco 7600 Optical Services Router Software Command Reference, 31 December 2001, Pages 28-29), *Sackett* (George Sackett, Interworking SNA with Cisco Solutions, Cisco Press, 19 February 1999, Pages 1-5) and The IEEE 802.1Q Standard (Author Unknown, IEEE standards for local and metropolitan area networks: virtual bridged local area networks, IEEE Std 802.1Q-1998, 8 March 1999, Pages 146-147).

Regarding claim 26, *Edsall* discloses a method in an access network for forcing a plurality of hosts connected to the access network to communicate through the access network rather than directly with each other, said access network comprising an access router and one or more switches, wherein the hosts are in communication contact with the access router via the switches, said method comprising the steps of:

a. Configuring in each switch, at least one port-based uplink Virtual Local Area Network (VLAN) for carrying uplink traffic, wherein each uplink VLAN is dedicated to a single host, and each host is associated with a different switch port of the switch (Column 4, Lines 39-45 and Claim 1 and Figures 1 and 2). (The system of *Edsall* discloses a switch that may have an arbitrary number of connected community or isolated VLANs. Each of the Isolated VLANs is uniquely associated with a single port on the switch and each port

of the switch is connected to a host server [Fig. 1 and Column 3, Line 43 to Column 4 Line 64]. *Edsall* further discloses that in one embodiment, each port comprises an isolated port, thereby creating a port that connects to a single host device to a single port associated with a single isolated VLAN [Column 5, Lines 47-49].)

b. Defining in the switches, a downlink VLAN, said downlink VLAN for carrying downlink traffic from the access router to the plurality of hosts, said downlink VLAN being common to all of the hosts connected to the access network (Abstract and Column 4, Lines 21-64). (The system of *Edsall* configures a common primary VLAN/Asymmetric Downlink VLAN that connects to all users of the switch [Column 4, Lines 21-64)]. Traffic is received from the access router/L3/L4 Device via the promiscuous port and is then sent to the appropriate user in the access network via the primary VLAN. The VLAN carries traffic coming from the router and going to the hosts, therefore, the asymmetric VLAN is for carrying downlink traffic from the hosts to the access router.)

c. Configuring the VLANs such that the hosts connected to the access network belong to the same IP subnet (Column 6, Lines 58-67). (The system of *Edsall* assigns the primary VLAN/Asymmetric Downlink VLAN to a single IP subnet, therefore all the hosts in the primary VLAN [which forms the access network] belong to the same subnet [Column 6, Lines 58-67].)

c. Forcing the switches to route traffic from the hosts through the access network, said forcing step comprising the VLANs forcing the switches to route uplink traffic from the hosts to the access router and subsequently forwarding by the access router, packets

received from the first host to the second host (Column 6, Lines 58-67). (All uplink traffic form the hosts must pass though the router, as direct communication among the hosts is prohibited by the isolated uplink VLAN status [Column 6, Lines 58-67].)

Edsall fails to disclose a method further comprising forcing the switches to route traffic from a first host to a second host in the same IP subnet through the access router, said forcing step comprising configuring the access router as a modified Address Resolution Protocol (ARP) proxy, wherein when the access router receives an ARP request from the first host requesting the MAC address of the second host and subsequently forwarding by the access router, packets received from the first host to the second host. In the same field of endeavor, The Cisco 7600 Optical Services Router Software Command Reference ("The 7600 command reference") discloses a method further comprising forcing the switches to route traffic from a first host to a second host in the same IP subnet through the access router, said forcing step comprising configuring the access router as a modified Address Resolution Protocol (ARP) proxy, wherein when the access router receives an ARP request from the first host requesting the MAC address of the second host and subsequently forwarding by the access router, packets received from the first host to the second host (ip local-proxy-arp command, Pages 28-29). (The local-proxy-ARP command is used to forward traffic between hosts on the same subnet when no routing is normally required.)

Therefore, since The 7600 Command Reference discloses the use of a local proxy ARP to enable communications between hosts on the same subnet that are otherwise unable to communicate, it would have been obvious to a person of ordinary skill in the art at the time of the invention to implement the local proxy ARP of The 7600 Command Reference into the teachings of *Edsall* to thereby enable the forced routing of inter-host traffic through the router.

The local proxy ARP of The 7600 Command Reference can be combined with the system of *Edsall* by setting up the VLANs as specified by *Edsall*, such that all traffic to and from the hosts is forced through the router, and then using local proxy ARP as taught by The 7600 Command Reference to enable communications between the different hosts. The motive to combine is to allow communication among the hosts that would otherwise be isolated by the VLANs, which generally prevent communication of the host devices at the link layer.

Edsall as modified by The Cisco 7600 Optical Services Router Software Command Reference does not explicitly disclose a method wherein the access router returns to the first host, the MAC address of the access router (The Office contends that such a disclosure is implicit in the use of local proxy ARP in a Cisco System. Assuming, arguendo, that it is not, the following reference is also supplied). In the same field of endeavor, *Sackett* discloses a method wherein the access router returns to the first host, the MAC address of the access router (Fig. 4-7, Page 4, "OriginMAC=A02EF0112480"). (The system of *Sackett* discloses that the ARP reply from a Cisco device implementing proxy ARP functionality is sent from the source MAC address [i.e. origin MAC] of the ARP Server/Router [Fig. 4-7, Page 4, "OriginMAC=A02EF0112480"]).

Therefore, since *Sackett* discloses the use of an ARP reply with a source MAC equal to the MAC address of the ARP server [i.e. Router in the system of *Edsall*], it would have been obvious to a person of ordinary skill in the art at the time of the invention to implement the MAC sourcing of *Sackett* into the teachings of *Edsall* by having the ARP proxy/router respond to an ARP request with a packet bearing the source MAC address of the router. The motive to combine is to guarantee that the host transmits packets directly to the router instead of sending packets to an incorrect MAC address, a further motive to combine is to provide additional security in the network by preventing hosts from learning the MAC address of other hosts on the network.

Finally, *Edsall* fails to disclose a method further comprising at least one port-based uplink Virtual Local Area Network (VLAN) for carrying uplink traffic to the access router and one asymmetric downlink VLAN, said downlink VLAN for carrying downlink traffic from the access router to the plurality of hosts, said downlink VLAN being common to all of the hosts connected to the access network. In the same field of endeavor, The IEEE 802.1Q Specification discloses a method further comprising at least one port-based uplink Virtual Local Area Network (VLAN) for carrying uplink traffic to the access router and one asymmetric downlink VLAN, said downlink VLAN for carrying downlink traffic from the access router to the plurality of hosts, said downlink VLAN being common to all of the hosts connected to the access network (Pages 146-147, Section B.1.3). (The IEEE 802.1Q Specification discloses the use of asymmetric VLANs to allow devices to access a central resource [In the case of the example, a central server] while prohibiting direct device communications. Each of the devices is assigned a unique uplink VLAN to connect to the central device [i.e. the red and blue VLANS for clients A and B] but utilizes a common downlink VLAN to receive traffic from the central device [i.e. The purple VLAN]. The *IEEE* 802.1Q Specification further discloses that although the figure shows only a single switch/bridge, traffic may flow through multiple intermediate devices [See NOTE, Page 147].)

Therefore, since The IEEE 802.1Q Specification suggests the use of individual asymmetric uplink VLANs and shared asymmetric downlink VLANs crossing multiple switches/intermediate devices to enable individual devices to reach a central resource while prohibiting direct device communication, it would have been obvious to a person of ordinary skill in the art that the non-hierartical VLANs of The IEEE 802.1Q Specification could likewise be used to access a different central resource [i.e. a router] while maintaining user isolation therefore leading a person of ordinary skill in the art to implement the non tiered VLANs of The IEEE 802.1Q Specification into the teachings of *Edsall* by using the primary VLAN only for

downlink traffic while using the isolated VLANs for uplink traffic. The motive to combine is to implement VLAN isolation in small access systems using a standard 802.1Q VLAN tagging thereby reducing system complexity. (i.e. when the number of users in a system is less then 4096, there is no need to use the tiered VLANs of the system of *Edsall* [See *Edsall*, Column 1, Lines 54-62], as each user may be assigned an individual VLAN without conflicting with any other user, and the overall complexity of the system may thereby be reduced by requiring all switches and the router to understand only simple 802.1Q VLAN tagging methods.) (Such a combination is also further supported the rationale of KSR v. Teleflex, as the claimed technique of using Asymmetric VLANs to separate user traffic was well known for improving a particular class of devices [i.e. connections to central servers] and was a part of the capabilities of a person of ordinary skill in the art and could readily have been applied by a person of ordinary skill in the art to a well known comparable device [i.e. a router which, like a server, is a central point for user access] to produce the predictable result of isolated VLAN access to the central router [See KSR International Co. v. Teleflex Inc., 127. S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007)].)

Regarding claim 27, *Edsall* discloses a system for forcing a plurality of hosts connected to an access network to communicate with each other through the access network rather than directly with each other, said system comprising:

a. An access router for providing the hosts with access to the access network (Fig. 1, Element 143).

b. At least one intermediate switch connected between the hosts and the access router, (Fig. 1, Element 102) said at least one switch comprising:

i. Means for configuring in the switch, at least one port-based uplink Virtual Local Area Network (VLAN) for carrying uplink traffic, wherein each, uplink VLAN is dedicated to a single host, and each host is associated with a different switch port of the switch (Column 4, Lines 39-45 and Claim 1 and Figures 1 and 2). (The system of *Edsall* discloses a switch that may have an arbitrary number of connected community or isolated VLANs. Each of the Isolated VLANs is uniquely associated with a single port on the switch and each port of the switch is connected to a host server [Fig. 1 and Column 3, Line 43 to Column 4 Line 64]. *Edsall* further discloses that in one embodiment, each port comprises an isolated port, thereby creating a port that connects to a single host device to a single port associated with a single isolated VLAN [Column 5, Lines 47-49].)

ii. Means for configuring a single downlink VLAN for carrying downlink traffic from the access router to the hosts, wherein the downlink VLAN is common to all of the hosts connected to the access network (Abstract and Column 4, Lines 21-64). (The system of *Edsall* configures a common primary VLAN/Asymmetric Downlink VLAN that connects to all users of the switch [Column 4, Lines 21-64)]. Traffic is received from the access router/L3/L4 Device via the promiscuous port and is then sent to the appropriate user in the access network via the primary VLAN. The VLAN carries traffic coming from the router and going to the hosts, therefore, the asymmetric VLAN is for carrying downlink traffic from the hosts to the access router.)

iii. Means for configuring the VLANs such that all of the hosts belong to the same IP subnet (Column 6, Lines 58-67). (The system of *Edsall* assigns the primary VLAN/Asymmetric Downlink VLAN to a single IP subnet, therefore all the hosts in the primary VLAN [which forms the access network] belong to the same subnet [Column 6, Lines 58-67].)

c. Wherein the system forces the switches to route traffic from the hosts through the access network, said forcing step comprising the VLANs forcing the switches to route uplink traffic from the hosts to the access router and wherein the sysetm further comprises means for subsequently forwarding by the access router, packets received from the first host to the second host (Column 6, Lines 58-67). (All uplink traffic form the hosts must pass though the router, as direct communication among the hosts is prohibited by the isolated uplink VLAN status [Column 6, Lines 58-67].)

Edsall fails to disclose system wherein the access router includes a modified Address Resolution Protocol (ARP) proxy agent, wherein when the access router receives an ARP request from a first host requesting the MAC address of a second host in the same IP subnet, the access router returns a response to the first host. In the same field of endeavor, The Cisco 7600 Optical Services Router Software Command Reference ("The 7600 command reference") discloses a modified Address Resolution Protocol (ARP) proxy agent, wherein when the access router receives an ARP request from a first host requesting the MAC address of a second host in the same IP subnet, the access router returns a response to the first host and a means for subsequently forwarding by the access router, packets received from the first host to the second

host (ip local-proxy-arp command, Pages 28-29). (The local-proxy-ARP command is used to forward traffic between hosts on the same subnet when no routing is normally required.)

Therefore, since The 7600 Command Reference discloses the use of a local proxy ARP to enable communications between hosts on the same subnet that are otherwise unable to communicate, it would have been obvious to a person of ordinary skill in the art at the time of the invention to implement the local proxy ARP of The 7600 Command Reference into the teachings of *Edsall* to thereby enable the forced routing of inter-host traffic through the router. The local proxy ARP of The 7600 Command Reference can be combined with the system of *Edsall* by setting up the VLANs as specified by *Edsall*, such that all traffic to and from the hosts is forced through the router, and then using local proxy ARP as taught by The 7600 Command Reference to enable communications between the different hosts. The motive to combine is to allow communication among the hosts that would otherwise be isolated by the VLANs, which generally prevent communication of the host devices at the link layer.

Edsall as modified by The Cisco 7600 Optical Services Router Software Command Reference does not explicitly disclose a system wherein the access router returns to the first host, the MAC address of the access router (The Office contends that such a disclosure is implicit in the use of local proxy ARP in a Cisco System. Assuming, arguendo, that it is not, the following reference is also supplied). In the same field of endeavor, *Sackett* discloses a system wherein the access router returns to the first host, the MAC address of the access router (Fig. 4-7, Page 4, "OriginMAC=A02EF0112480"). (The system of *Sackett* discloses that the ARP reply from a Cisco device implementing proxy ARP functionality is sent from the source MAC address [i.e. origin MAC] of the ARP Server/Router (Fig. 4-7, Page 4, "OriginMAC=A02EF0112480").

Therefore, since *Sackett* discloses the use of an ARP reply with a source MAC equal to the MAC address of the ARP server [i.e. Router in the system of *Edsall*], it would have been

obvious to a person of ordinary skill in the art at the time of the invention to implement the MAC sourcing of *Sackett* into the teachings of *Edsall* by having the ARP proxy/router respond in a response packet bearing the source MAC address of the router. The motive to combine is to guarantee that the host transmits all packets directly to the router, a further motive to combine is to provide additional security in the network by preventing hosts from learning the MAC address of other hosts on the network.

Finally, *Edsall* fails to disclose a system further comprising means for configuring in the switch, at least one port-based uplink Virtual Local Area Network (VLAN) for carrying uplink traffic to the access router, wherein each, uplink VLAN is dedicated to a single host, and each host is associated with a different switch port of the switch and means for configuring a single asymmetric downlink VLAN for carrying downlink traffic from the access router to the hosts, wherein the downlink VLAN is common to all of the hosts connected to the access network. In the same field of endeavor, The IEEE 802.1Q Specification discloses a system further comprising means for configuring in the switch, at least one port-based uplink Virtual Local Area Network (VLAN) for carrying uplink traffic to the access router, wherein each, uplink VLAN is dedicated to a single host, and each host is associated with a different switch port of the switch and means for configuring a single asymmetric downlink VLAN for carrying downlink traffic from the access router to the hosts, wherein the downlink VLAN is common to all of the hosts connected to the access network (Pages 146-147, Section B.1.3). (The IEEE 802.1Q Specification discloses the use of asymmetric VLANs to allow devices to access a central resource [In the case of the example, a central server] whole prohibiting direct device communications. Each of the devices is assigned a unique uplink VLAN to connect to the central device [i.e. the red and blue VLANS for clients A and B] but utilizes a common downlink VLAN to receive traffic from the central device [i.e. The purple VLAN]. The *IEEE* 802.1Q

Specification further discloses that although the figure shows only a single switch/bridge, traffic may flow through multiple intermediate devices [See NOTE, Page 147].)

Therefore, since The IEEE 802.1Q Specification suggests the use of individual asymmetric uplink VLANs and shared asymmetric downlink VLANs crossing multiple switches/intermediate devices to enable individual devices to reach a central resource while prohibiting direct device communication, it would have been obvious to a person of ordinary skill in the art that the non-hierartical VLANs of The IEEE 802.1Q Specification could likewise be used to access a different central resource [i.e. a router] while maintaining user isolation therefore leading a person of ordinary skill in the art to implement the non tiered VLANs of The IEEE 802.1Q Specification into the teachings of *Edsall* by using the primary VLAN only for downlink traffic while using the isolated VLANs for uplink traffic. The motive to combine is to implement VLAN isolation in small access systems using a standard 802.1Q VLAN tagging thereby reducing system complexity. (i.e. when the number of users in a system is less then 4096, there is no need to use the tiered VLANs of the system of *Edsall* [See *Edsall*, Column 1, Lines 54-62], as each user may be assigned an individual VLAN without conflicting with any other user, and the overall complexity of the system may thereby be reduced by requiring all switches and the router to understand only simple 802.1Q VLAN tagging methods.) (Such a combination is also further supported the rationale of KSR v. Teleflex, as the claimed technique of using Asymmetric VLANs to separate user traffic was well known for improving a particular class of devices [i.e. connections to central servers] and was a part of the capabilities of a person of ordinary skill in the art and could readily have been applied by a person of ordinary skill in the art to a well known comparable device [i.e. a router which, like a server, is a central point for user access] to produce the predictable result of isolated VLAN access to the central

router [See KSR International Co. v. Teleflex Inc., 127. S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007)].)

4. **Claims 10, 11, 21 and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over *Edsall*, et al. (US Patent No. 6,741,592 B1), The Cisco 7600 Optical Services Router Software Command Reference (Author Unknown, The Cisco 7600 Optical Services Router Software Command Reference, 31 December 2001, Pages 28-29), *Sackett* (George Sackett, Interworking SNA with Cisco Solutions, Cisco Press, 19 February 1999, Pages 1-5) and The IEEE 802.1Q Standard (Author Unknown, IEEE standards for local and metropolitan area networks: virtual bridged local area networks, IEEE Std 802.1Q-1998, 8 March 1999, Pages 146-147) as applied to claims 26 and 27, Supra, and further in view of *Sistanizadeh*, et al. (US Patent No. 6,101,182).

Regarding claims 10 and 21, *Edsall* fails to disclose a method and system further comprising retrieving by the access router, address mapping information for the hosts during a user authentication procedure. In the same field of endeavor, *Sistanizadeh* discloses a method and system further comprising retrieving by the access router, address mapping information for the hosts during a user authentication procedure (Figure 1, Element address mapping information for the hosts during the user authentication procedure (Column 18, Lines 4-9).

Therefore, since *Sistanizadeh* suggests the retrieving of address mapping information by the access router during authentication, it would have been obvious to one of ordinary skill in the art at the time of the invention to apply a method and apparatus for retrieving of address mapping information by the access router during authentication as disclosed by *Sistanizadeh* into the teachings of *Edsall*. The address mapping of *Sistanizadeh* can be combined with the

system of *Edsall* by having the router of *Edsall* return the IP address assigned to the user during user authentication, as taught by *Sistanizadeh*. The motive to combine is to enable the use of address assignment and authentication, thereby improving security.

Regarding claims 11 and 22, *Edsall* fails to disclose a method and system further comprising retrieving by the access router, address mapping information for the hosts during an IP allocation procedure. In the same field of endeavor, *Sistanizadeh* discloses a method and system further comprising retrieving by the access router, address mapping information for the hosts during an IP allocation procedure (Figure 1, Element address mapping information for the hosts during the during the IP allocation procedure (Column 18, Lines 4-9).

Therefore, since *Sistanizadeh* suggests the retrieving of address mapping information by the access router during authentication, it would have been obvious to one of ordinary skill in the art at the time of the invention to apply a method and apparatus for retrieving of address mapping information by the access router during authentication as disclosed by *Sistanizadeh* into the teachings of *Edsall*. The address mapping of *Sistanizadeh* can be combined with the system of *Edsall* by having the router of *Edsall* return the IP address assigned to the user during user authentication, as taught by *Sistanizadeh*. The motive to combine is to enable the use of address assignment and authentication, thereby improving security.

5. **Claims 12 and 23** are rejected under 35 U.S.C. 103(a) as being unpatentable over *Edsall*, et al. (US Patent No. 6,741,592 B1), The Cisco 7600 Optical Services Router Software Command Reference (Author Unknown, The Cisco 7600 Optical Services Router Software Command Reference, 31 December 2001, Pages 28-29), *Sackett* (George Sackett, Interworking SNA with Cisco Solutions, Cisco Press, 19 February 1999, Pages 1-5) and The IEEE 802.1Q Standard (Author Unknown, IEEE standards for local and metropolitan area

networks: virtual bridged local area networks, IEEE Std 802.1Q-1998, 8 March 1999, Pages 146-147) as applied to claims 26 and 27, Supra, and further in view of *Yamaya*, et al. (US Pre Grant Publication No. 2002/0184387).

Regarding claims 12 and 23, *Edsall* fails to disclose a method and system further comprising providing more than one access router in the access network, the VLANs being configured such that the access routers belong to the same VLANs. In the same field of endeavor, *Yamaya* discloses providing more than one access router in the access network, the VLANs being configured such that the access routers belong to the same VLANs (Figure 15, Elements 10 and 11 and Paragraph 0131).

Therefore, since *Yamaya* suggests the use of redundant routers on the same VLAN it would have been obvious to one of ordinary skill in the art at the time of the invention to apply a method and apparatus for the use of redundant routers on the same VLAN as disclosed by *Yamaya* into the teachings of *Edsall*. The redundant router of *Yamaya* can be combined with the system of *Edsall* by providing multiple routers connected to different ports of the switch of *Edsall* each operating on the same VLANs to provide redundancy, as taught by *Yamaya*. The motive to combine is provided by *Yamaya* and is to provide backup in case one router fails (Paragraph 0002).

6. **Claims 28 and 29** are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 3069 (D. McPherson and B. Dykes, Request For Comments 3069, February 2001, Pages 1-7) in view of The Cisco 7600 Optical Services Router Software Command Reference (Author Unknown, The Cisco 7600 Optical Services Router Software Command Reference, 31 December 2001, Pages 28-29), *Sackett* (George Sackett, Interworking SNA with Cisco

Solutions, Cisco Press, 19 February 1999, Pages 1-5) and The IEEE 802.1Q Standard (Author Unknown, IEEE standards for local and metropolitan area networks: virtual bridged local area networks, IEEE Std 802.1Q-1998, 8 March 1999, Pages 146-147).

Regarding claim 28, RFC 3069 discloses a method in an access network for forcing a plurality of hosts connected to the access network to communicate through the access network rather than directly with each other, said access network comprising an access router and one or more switches, wherein the hosts are in communication contact with the access router via the switches, said method comprising the steps of:

a. Configuring in each switch, at least one port-based Virtual Local Area Network (VLAN) for carrying both uplink traffic and downlink unicast traffic, wherein each VLAN is dedicated to a single customer VLAN (Pages 3-5, Section 2, Discussion). (The system of RFC 3069 utilizes sub-VLANs to isolate customers connected to ports on a common switch [Pages 3-5, Section 2, Discussion]. Each of the separate sub-VLANs prevents communication between the customers, except via the router, which acts as a proxy ARP server to direct traffic between the subnets [Pages 3-5, Section 2, Discussion].)

b. Configuring the VLANs such that the hosts connected to the access network belong to the same IP subnet (Page 4, Table 2). (The system of RFC 3069 discloses that all members on a single super-net [i.e. access network] linking each user to the switch are assigned a common IP subnet [Pages 3-5, Section 2, Discussion].)

c. Configuring the access router as a modified Address Resolution Protocol (ARP) proxy wherein when the access router receives an ARP request from a first host requesting the MAC address of a second host in the same IP subnet and replies to the ARP request and subsequently forwarding by the access router, packets received from the first host to the second host (Page 3, First and Second Paragraph).

RFC 3069 fails to disclose a method further comprising configuring the access router as a modified Address Resolution Protocol (ARP) proxy, wherein when the access router receives an ARP request from a first host requesting the MAC address of a second host in the same IP subnet, the access router responds to the first host, and subsequently forwarding by the access router, packets received from the first host to the second host. In the same field of endeavor, The Cisco 7600 Optical Services Router Software Command Reference ("The 7600 command reference") discloses a method further comprising forcing the switches to route traffic from a first host to a second host in the same IP subnet through the access router, said forcing step comprising configuring the access router as a modified Address Resolution Protocol (ARP) proxy, wherein when the access router receives an ARP request from the first host requesting the MAC address of the second host and subsequently forwarding by the access router, packets received from the first host to the second host (ip local-proxy-arp command, Pages 28-29). (The local-proxy-ARP command is used to forward traffic between hosts on the same subnet when no routing is normally required.)

Therefore, since The 7600 Command Reference discloses the use of a local proxy ARP to enable communications between hosts on the same subnet that are otherwise unable to communicate, it would have been obvious to a person of ordinary skill in the art at the time of the invention to implement the local proxy ARP of The 7600 Command Reference into the

teachings of RFC 3069 to thereby enable the forced routing of inter-host traffic through the router. The local proxy ARP of The 7600 Command Reference can be combined with the system of RFC 3069 by setting up the VLANs as specified by RFC 3069, such that all traffic to and from the hosts is forced through the router, and then using local proxy ARP as taught by The 7600 Command Reference to enable communications between the different hosts. The motive to combine is to allow communication among the hosts that would otherwise be isolated by the VLANs, which generally prevent communication of the host devices at the link layer.

RFC 3069 as modified by The Cisco 7600 Optical Services Router Software Command Reference does not explicitly disclose a method wherein the access router returns to the first host, the MAC address of the access router (The Office contends that such a disclosure is implicit in the use of local proxy ARP in a Cisco System. Assuming, arguendo, that it is not, the following reference is also supplied). In the same field of endeavor, *Sackett* discloses a method wherein the access router returns to the first host, the MAC address of the access router (Fig. 4-7, Page 4, "OriginMAC=A02EF0112480"). (The system of *Sackett* discloses that the ARP reply from a Cisco device implementing proxy ARP functionality is sent from the source MAC address [i.e. origin MAC] of the ARP Server/Router (Fig. 4-7, Page 4, "OriginMAC=A02EF0112480").

Therefore, since *Sackett* discloses the use of an ARP reply with a source MAC equal to the MAC address of the ARP server [i.e. Router in the system of RFC 3069], it would have been obvious to a person of ordinary skill in the art at the time of the invention to implement the MAC sourcing of *Sackett* into the teachings of RFC 3069 by having the ARP proxy/router respond to an ARP request a packet bearing the source MAC address of the router. The motive to combine is to guarantee that the host transmits packets directly to the router instead of sending packets to an incorrect MAC address, a further motive to combine is to provide additional security in the network by preventing hosts from learning the MAC address of other hosts on the network.

Finally, RFC 3069 fails to disclose a method further comprising configuring in each switch, at least one port-based Virtual Local Area Network (VLAN) for carrying both uplink traffic and downlink unicast traffic between the access router and individual hosts connected to the switch, wherein each VLAN is dedicated to a single host, and each host is associated with a different switch port of the switch. In the same field of endeavor, The IEEE 802.1Q Specification discloses a method further comprising configuring in each switch, at least one port-based Virtual Local Area Network (VLAN) for carrying both uplink traffic and downlink unicast traffic between the access router and individual hosts connected to the switch, wherein each VLAN is dedicated to a single host, and each host is associated with a different switch port of the switch (Pages 144-146 and Figure B-2). (The IEEE 802.1Q Specification discloses the use of an isolated VLAN for each client device connected to a switch port [i.e. The Red and Blue VLANs for the first and second clients, respectively]. The isolated VLANS are utilized for both uplink and downlink traffic and further connect each client to the router [Pages144-146 and Figure B-2].)

Therefore, since The IEEE 802.1Q Specification suggests the use of per client and port VLANs to connect to a central router, it would have been obvious to a person of ordinary skill in the art implement the non-hierartical VLANs of The IEEE 802.1Q Specification into the teachings of RFC 3069 by connecting a client to each port and assigning each client an individual VLAN for communicating with the switch. The motive to combine is to simplify the system where less the 4096 clients are to be connected, by eliminating the use of unnecessary primary and sub VLANs and using individual 802.1Q compliant VLANs for each client. (Such a combination is also further supported the rationale of KSR v. Teleflex, as the claimed technique of using VLANs to separate user traffic was well known for improving a particular class of devices [i.e. connections to central servers] and was a part of the capabilities of a person of ordinary skill in the art and could readily have been applied by a person of ordinary skill in the

art to a well known comparable device [i.e. a router which, like a server, is a central point for user access] to produce the predictable result of isolated VLAN access to the central router [See KSR International Co. v. Teleflex Inc., 127. S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007)].)

Regarding claim 29, RFC 3069 discloses a system for forcing a plurality of hosts connected to an access network to communicate with each other through the access network rather than directly with each other, said system comprising an access router for providing the hosts with access to the access network and at least one intermediate switch connected between the hosts and the access router, said at least one switch comprising:

a. Means for configuring in the switch, at least one port-based Virtual Local Area Network (VLAN) for carrying both uplink traffic and downlink unicast traffic, wherein each VLAN is dedicated to a single customer (Pages 3-5, Section 2, Discussion). (The system of RFC 3069 utilizes sub-VLANs to isolate customers connected to ports on a common switch [Pages 3-5, Section 2, Discussion]. Each of the separate sub-VLANs prevents communication between the customers, except via the router, which acts as a proxy ARP server to direct traffic between the subnets [Pages 3-5, Section 2, Discussion].)

b. Means for configuring the VLANs such that all of the hosts belong to the same IP subnet (Page 4, Table 2). (The system of RFC 3069 discloses that all members on a single super-net [i.e. access network] linking each user to the switch are assigned a common IP subnet [Pages 3-5, Section 2, Discussion].)

c. Wherein the access router includes a modified Address Resolution Protocol (ARP) proxy agent, wherein when the access router receives an ARP request from a first host requesting the MAC address of a second host in the same IP subnet, the access router responds to the ARP request and a means for subsequently forwarding by the access router, packets received from the first host to the second host (Page 3, First and Second Paragraph).

RFC 3069 fails to disclose a system wherein the access router includes a modified Address Resolution Protocol (ARP) proxy agent, wherein when the access router receives an ARP request from a first host requesting the MAC address of a second host in the same IP subnet, the access router responds to the first host and further comprising a means for subsequently forwarding by the access router, packets received from the first host to the second host. In the same field of endeavor, The Cisco 7600 Optical Services Router Software Command Reference ("The 7600 command reference") discloses a system wherein the access router includes a modified Address Resolution Protocol (ARP) proxy agent, wherein when the access router receives an ARP request from a first host requesting the MAC address of a second host in the same IP subnet, the access router responds to the first host and further comprising a means for subsequently forwarding by the access router, packets received from the first host to the second host (ip local-proxy-arp command, Pages 28-29). (The local-proxy-ARP command is used to forward traffic between hosts on the same subnet when no routing is normally required.)

Therefore, since The 7600 Command Reference discloses the use of a local proxy ARP to enable communications between hosts on the same subnet that are otherwise unable to communicate, it would have been obvious to a person of ordinary skill in the art at the time of

the invention to implement the local proxy ARP of The 7600 Command Reference into the teachings of RFC 3069 to thereby enable the forced routing of inter-host traffic through the router. The local proxy ARP of The 7600 Command Reference can be combined with the system of RFC 3069 by setting up the VLANs as specified by RFC 3069, such that all traffic to and from the hosts is forced through the router, and then using local proxy ARP as taught by The 7600 Command Reference to enable communications between the different hosts. The motive to combine is to allow communication among the hosts that would otherwise be isolated by the VLANs, which generally prevent communication of the host devices at the link layer.

RFC 3069 as modified by The Cisco 7600 Optical Services Router Software Command Reference does not explicitly disclose a system wherein when the access router receives an ARP request from a first host requesting the MAC address of a second host in the same IP subnet, the access router returns to the first host, the MAC address of the access router (The Office contends that such a disclosure is implicit in the use of local proxy ARP in a Cisco System. Assuming, arguendo, that it is not, the following reference is also supplied). In the same field of endeavor, *Sackett* discloses a system wherein when the access router receives an ARP request from a first host requesting the MAC address of a second host in the same IP subnet, the access router returns to the first host, the MAC address of the access router (Fig. 4-7, Page 4, "OriginMAC=A02EF0112480"). (The system of *Sackett* discloses that the ARP reply from a Cisco device implementing proxy ARP functionality is sent from the source MAC address [i.e. origin MAC] of the ARP Server/Router (Fig. 4-7, Page 4, "OriginMAC=A02EF0112480").

Therefore, since *Sackett* discloses the use of an ARP reply with a source MAC equal to the MAC address of the ARP server [i.e. Router in the system of RFC 3069], it would have been obvious to a person of ordinary skill in the art at the time of the invention to implement the MAC sourcing of *Sackett* into the teachings of RFC 3069 by having the ARP proxy/router respond to

an ARP request a packet bearing the source MAC address of the router. The motive to combine is to guarantee that the host transmits packets directly to the router instead of sending packets to an incorrect MAC address, a further motive to combine is to provide additional security in the network by preventing hosts from learning the MAC address of other hosts on the network.

Finally, RFC 3069 fails to disclose a system further comprising means for configuring in the switch, at least one port-based Virtual Local Area Network (VLAN) for carrying both uplink traffic and downlink unicast traffic between the access router and individual hosts connected to the switch, wherein each VLAN is dedicated to a single host, and each host is associated with a different switch port of the switch. In the same field of endeavor, The IEEE 802.1Q Specification discloses a system further comprising means for configuring in the switch, at least one port-based Virtual Local Area Network (VLAN) for carrying both uplink traffic and downlink unicast traffic between the access router and individual hosts connected to the switch, wherein each VLAN is dedicated to a single host, and each host is associated with a different switch port of the switch (Pages 144-146 and Figure B-2). (The IEEE 802.1Q Specification discloses the use of an isolated VLAN for each client device connected to a switch port [i.e. The Red and Blue VLANs for the first and second clients, respectively]. The isolated VLANS are utilized for both uplink and downlink traffic and further connect each client to the router [Pages144-146 and Figure B-2].)

Therefore, since The IEEE 802.1Q Specification suggests the use of per client and port VLANs to connect to a central router, it would have been obvious to a person of ordinary skill in the art implement the non-hierartical VLANs of The IEEE 802.1Q Specification into the teachings of RFC 3069 by connecting a client to each port and assigning each client an individual VLAN for communicating with the switch. The motive to combine is to simplify the system where less the 4096 clients are to be connected, by eliminating the use of unnecessary

primary and sub VLANs and using individual 802.1Q compliant VLANs for each client. (Such a combination is also further supported the rationale of KSR v. Teleflex, as the claimed technique of using VLANs to separate user traffic was well known for improving a particular class of devices [i.e. connections to central servers] and was a part of the capabilities of a person of ordinary skill in the art and could readily have been applied by a person of ordinary skill in the art to a well known comparable device [i.e. a router which, like a server, is a central point for user access] to produce the predictable result of isolated VLAN access to the central router [See KSR International Co. v. Teleflex Inc., 127. S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007)].)

Prior Art made of Record and not Relied Upon

The following prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. *Kalintsev*, et al. (D. Kalintsev, J. Schlyter and J. Desmaranis, "6500/IOS + CatOS HSRP + local-proxy-arp problem", 6 June 2001 to 14 November 2001, Pages 1-6) - Disclosing the use of the Cisco local proxy arp command to enable inter-client communications in a system where customers are assigned to a common subnet but separated by private VLANs.

b. *Schlyter*, et al. (J. Schlyter and D. Kalintsev, pVLANs question, 6-7 June 2001, Pages 1-2) - Disclosing the use of the Cisco local proxy arp command to enable inter-client

communications in a system where customers are assigned to a common subnet but separated by private VLANs.

c. *Sanjay*, et al. (S. Sanjay and R. Perlman, Shared VLAN learning: What is it and why should we care?, 28-29 March 2007, Pages 1-5) – Demonstrating that the Cisco local proxy ARP command results in the transmission of packets between devices on the same subnet but different VLANs via the router (Page 1).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Crutchfield whose telephone number is (571) 270-3989. The examiner can normally be reached on Monday through Friday 8:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Daniel Ryman can be reached on (571) 272-3152. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher Crutchfield/
Examiner, Art Unit 2419
3/25/2009

/Daniel J. Ryman/
Supervisory Patent Examiner, Art Unit 2419